PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-332747
(43)Date of publication of application : 30.11.2000

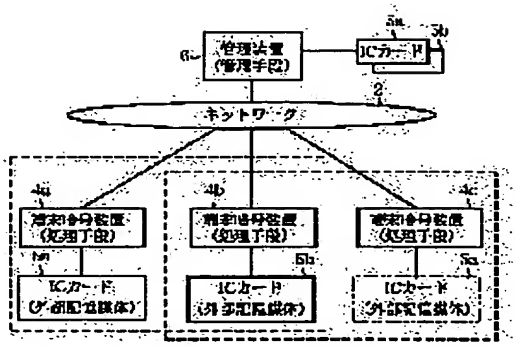
(51)Int.CI. H04L 9/32
H04L 9/08
H04L 12/46
H04L 12/28
H04L 12/56

(21)Application number : 11-142486
(22)Date of filing : 21.05.1999

(71)Applicant : MITSUBISHI ELECTRIC CORP
NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : BOKU BIJIYOU
WATANABE AKIRA
MIYAGAWA AKIKO
ATOZAWA SHINOBU
SAIJO TOMOYUKI
OKA KATSUYA
SEGUCHI ARIYOSHI

(54) CLOSED-AREA COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To allow different terminals to conduct the same closed area communication, even when a work site is changed by introducing external storage media to the title system so as to authenticate a user belonging to a prescribed group in the closed area communication.
SOLUTION: This closed-area communication system is configured with IC cards 5a, 5b that store information for user authentication which is an object of the closed area communication, a plurality of terminal encryption units 4a-4c, that encrypt communication data and decode the encrypted data according to contents of an operating table 13 produced on the basis of the information stored in the IC cards 5a, 5b, and a management unit 6 that is connected to the



terminal encipherment units 4a-4c via a network 2 and issues the IC cards 5a, 5b to a user which is an object of the closed-area communication.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－332747
（P2000－332747A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.⁷	識別記号	FI		テーマコード*(参考)
H04L 9/32		H04L 9/00	675D	5J104
9/08			601B	5K030
12/46			673E	5K033
12/28		11/00	310C	
12/56		11/20	102Z	

審査請求　未請求　請求項の数6　ＯＬ　（全９頁）

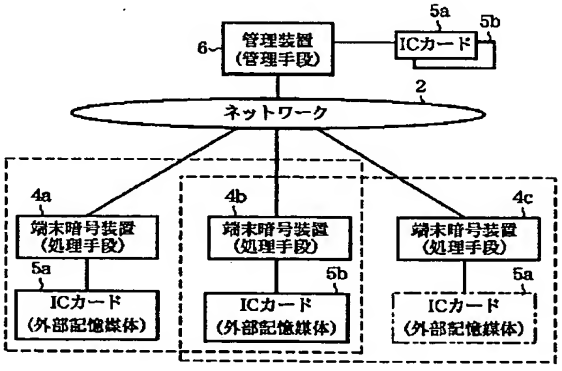
(21)出願番号　特願平11－142486
(22)出願日　平成11年５月21日(1999.5.21)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　朴　美娘
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100066474
弁理士　田澤　博昭　（外１名）

最終頁に続く

(54)【発明の名称】　閉域通信システム

(57)【要約】
【課題】　外部記憶媒体を導入して、所定のグループに属するユーザに対して閉域通信におけるユーザ認証を行うことにより、作業場所が変わっても、異なる端末より同一の閉域通信が行える閉域通信システムを得る。
【解決手段】　閉域通信の対象となるユーザ認証のための情報を保持するＩＣカード５ａ，５ｂと、このＩＣカード５ａ，５ｂに保持されている情報をもとに生成した動作テーブル１３の内容に従って、通信データの暗号および復号の処理を行う複数の端末暗号装置４ａ～４ｃと、ネットワーク２を介して端末暗号装置４ａ～４ｃに接続され、閉域通信の対象となるユーザに対して上記ＩＣカード５ａ，５ｂの発行を行う管理装置６とによって構成された閉域通信システムである。



1

【特許請求の範囲】

【請求項１】　所定のグループに属するユーザ間で閉域通信を行う際の、閉域通信の対象となるユーザ認証のための情報を保持する外部記憶媒体と、

ネットワークに接続され、前記外部記憶媒体に保持された前記ユーザ認証のための情報をもとに生成した動作テーブルの内容に従って通信データの暗号および復号の処理を行う複数の処理手段と、

前記外部記憶媒体を発行する、前記処理手段に前記ネットワークを介して接続される管理手段とを備えた閉域通信システム。

【請求項２】　外部記憶媒体に、閉域通信の対象となるユーザ認証のための情報として、ユーザＩＤ、認証秘密情報、管理手段情報を保持させ、

管理手段は、前記外部記憶媒体が処理手段に挿入されると、当該外部記憶媒体の保持する情報をもとに、閉域通信に必要な動作テーブルを前記処理手段に配送するものであることを特徴とする請求項１記載の閉域通信システム。

【請求項３】　管理手段は、ユーザのグループＩＤおよびそれに対応する暗号鍵を処理手段に配送するものであり、

前記処理手段は、それらの情報を通信相手の処理手段または中継装置との間で交換し、前記通信相手の処理手段との間の閉域通信に必要となる動作テーブルを自動生成するものであることを特徴とする請求項２記載の閉域通信システム。

【請求項４】　処理手段は、外部記憶媒体が抜き取られたことを検出すると、現在保持している動作テーブルを消去するものであることを特徴とする請求項２記載の閉域通信システム。

【請求項５】　管理手段は、外部記憶媒体を発行する際に、当該外部記憶媒体の内容をパスワードで暗号化するとともに、前記パスワードの初期パスワードの決定を行うものであり、

処理手段は、前記パスワードを変更するパスワード変更手段を有するものであることを特徴とする請求項２記載の閉域通信システム。

【請求項６】　外部記憶媒体としてＩＣカードを用いたことを特徴とする請求項１から請求項５のうちのいずれか１項記載の閉域通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、機密保護を目的とするネットワークシステムにおいて、所定のグループに属するユーザに対して閉域通信を提供する閉域通信システムに関するものである。

【０００２】

【従来の技術】図１１は、例えば特開平１１－０５５３２２の明細書および図面に示された、従来の閉域通信システムを示すシステム構成図である。図において、１ａ，１ｂ，１ｃは閉域通信を行う端末であり、２はこれらの端末１ａ～１ｃが収容されるネットワークである。３ａ，３ｂ，３ｃは端末１ａ～１ｃとネットワーク２の間の中継経路上に配置された暗号装置であり、暗号装置３ａはグループＩＤが１の暗号鍵、暗号装置３ｂはグループＩＤが１および２の暗号鍵、暗号装置３ｃはグループＩＤが２の暗号鍵をそれぞれ保有している。なお、上記端末１ａ～１ｃおよび暗号装置３ａ～３ｃはその各々を区別しない場合には、それぞれ端末１あるいは暗号装置３と表記する。

【０００３】図１２は上記暗号装置３の内部構成を示すブロック図である。図において、１０は暗号／復号処理部、１１は透過中継処理部、１２は廃棄処理部である。１３は通信データの処理方法を示す動作テーブル、１４は自動学習処理部である。なお、初期の時点の動作テーブル１３には、通信データの処理方法はなにも登録されていないものとする。１５はネットワーク２側のインタフェースであるパブリックポート、１６は端末１側のインタフェースであるローカルポート、１７，１８は送受信処理部である。

【０００４】次に動作について説明する。従来の閉域通信システムでは、ネットワーク２に収容されている通信端末１ａ～１ｃ間の中継経路上に配置された暗号装置３ａ～３ｃが保持するグループＩＤ情報を収集し、収集したグループＩＤ情報に対応した暗号鍵のＩＤ情報に基づいて動作テーブル１３を自動学習し、その学習結果に基づいて自動生成した動作テーブル１３を用いて通信するものである。ここで、各暗号装置３ａ～３ｃに割り当てられるグループＩＤおよび暗号鍵の実体はあらかじめ配送されており、各暗号装置３ａ～３ｃはそれらの情報を一組または複数組、動作テーブル１３に保持している。

【０００５】端末１ａと端末１ｂの間で閉域通信を行う場合、端末１ａから端末１ｂへの通信データは暗号装置３ａにおいて、その動作テーブル１３の内容に従って、暗号／復号処理部１０でＩＤが１の暗号鍵を用いて暗号化され、暗号化通信データとして端末１ｂ宛てに送信される。暗号装置３ｂでは暗号／復号処理部１０において、この暗号装置３ａからの暗号化通信データをその動作テーブル１３の内容に従って、元の通信データに復号し、それを端末１ｂへ送信する。同様に、端末１ｂから端末１ａへの通信データは、暗号装置３ｂでその動作テーブル１３の内容に従って、ＩＤが１の暗号鍵により暗号化されて暗号装置３ａへ送られ、その動作テーブル１３の内容に従って、ＩＤが１の暗号鍵により復号され、端末１ａに達する。

【０００６】なお、このような従来の閉域通信システムに関係のある技術が記載されている文献としては、この他にも、例えば特開平９－２４７１４１号公報、特開平１０－１７１７１７号公報などがある。

【０００７】
【発明が解決しようとする課題】従来の閉域通信システムは以上のように構成されているので、端末１ａ～１ｃ間の暗号通信を中継する暗号装置３ａ～３ｃにあらかじめ登録されているグループＩＤ、またはあらかじめ配送されているグループＩＤによる暗号鍵によって閉域通信を実現しているので、ユーザが使用する端末１ａ～１ｃが固定されてしまうという課題があった。
【０００８】この発明は、上記のような課題を解決するためになされたもので、外部記憶媒体を導入して、所定のグループに属するユーザに対して閉域通信におけるユーザ認証を行うことにより、作業場所が変わっても、異なる端末より同一の閉域通信が行える閉域通信システムを得ることを目的とする。
【０００９】
【課題を解決するための手段】この発明に係る閉域通信システムは、ユーザ認証のための情報を保持する外部記憶媒体をユーザに持たせ、当該情報をもとに生成した動作テーブルの内容に従って、通信データの暗号および復号の処理を行うことによって、異なる作業場所からでも同一の閉域通信ができるようにしたものである。
【００１０】この発明に係る閉域通信システムは、ユーザＩＤ、認証秘密情報、管理手段情報を保持した外部記憶媒体を処理手段に挿入したとき、管理手段より処理手段に対して、外部記憶媒体が保持する情報をもとに、閉域通信に必要な動作テーブルを配送するようにしたものである。
【００１１】この発明に係る閉域通信システムは、管理手段から処理手段に対して、ユーザのグループＩＤおよびそれに対応する暗号鍵を配送し、処理手段はそれらの情報を通信相手の処理手段または中継装置との間で交換して、動作テーブルの自動生成を行うようにしたものである。
【００１２】この発明に係る閉域通信システムは、外部記憶媒体の抜き取りを検出した処理手段が、保持している動作テーブルを消去するようにしたものである。
【００１３】この発明に係る閉域通信システムは、管理手段に、外部記憶媒体を発行する際に外部記憶媒体の内容をパスワードで暗号化する機能、および初期パスワードを決定する機能を持たせ、処理手段に、パスワードの変更を行う機能を持たせたものである。
【００１４】この発明に係る閉域通信システムは、ＩＣカードを外部記憶媒体として用いるようにしたものである。
【００１５】
【発明の実施の形態】以下、この発明の実施の一形態を説明する。
実施の形態１．図１は、この発明の実施の形態１による閉域通信システムの構成を示すシステム構成図である。図において、２は閉域通信を行う所定のグループのメンバであるユーザに対して、閉域通信を許容するネットワークであり、４ａ，４ｂ，４ｃはそれぞれこのネットワーク２に収容されて、ユーザが閉域通信を行う端末の機能と、閉域通信に先立って暗号鍵情報を自動学習し、通信データの暗号／復号処理を行う暗号装置の機能とを併せ持った、処理手段としての端末暗号装置である。５ａ，５ｂは閉域通信を行うユーザが所有し、それを所有しているユーザにのみ閉域通信を可能とするための情報が格納された、外部記憶媒体としてのＩＣカードであり、６は閉域通信を行うグループの登録を行い、当該グループのメンバである各ユーザにこのＩＣカード５ａ，５ｂを発行する管理手段としての管理装置である。なお、上記端末暗号装置４ａ～４ｃおよびＩＣカード５ａ，５ｂはその各々を区別しない場合には、それぞれ端末暗号装置４あるいはＩＣカード５と表記する。
【００１６】図２は上記端末暗号装置４の内部構成を示すブロック図である。図において、１０は通信データの暗号および復号処理を行う暗号／復号処理部である。１１は通信データをそのまま透過的に中継する透過中継処理部であり、１２は通信データを廃棄する廃棄処理部である。１３は通信データの処理方法を示す動作テーブルであり、通信データの宛先となる端末暗号装置４と送信元となる端末暗号装置４のペア毎に、当該通信データの処理方法が登録されるものである。なお、初期の時点では、この動作テーブル１３には送信データの処理方法は何も登録されていないものとする。１４はこの動作テーブル１３の自動学習処理部であり、動作テーブル１３に処理方法が登録されていない場合に起動されるものである。１５はネットワーク２側のインタフェースであるパブリックポートであり、１７，１８は通信データの受信処理および送信処理を実施する送受信処理部である。なお、これら各部は、図１２に同一符号を付して示した従来のそれらに相当する部分である。
【００１７】また、１９は閉域通信を行うユーザによってＩＣカード５が挿入され、当該ＩＣカード５に保持されている閉域通信を可能とするための情報の読み取りが行われるＩＣカードリーダである。２０はユーザによるこのＩＣカードリーダ１９へのＩＣカード５の挿抜を常に監視しながら、ＩＣカード５より読み出された情報を処理するＩＣカード処理部であり、このＩＣカード処理部２０はＩＣカード５の内容を暗号化するためのパスワードを変更するパスワード変更手段としても機能する。２１は従来のローカルポートの部分に配置されたＰＣＩ／Ｆであり、この端末暗号装置４とユーザとのマン・マシンのインタフェースをとるものである。なお、ＩＣカード処理部２０はこのＰＣＩ／Ｆ２１と送受信処理部１８の接続点に、ＩＣカードリーダ１９が読み出した情報を処理して出力している。
【００１８】図３は管理装置６によってユーザに発行されるＩＣカード５に書き込まれる情報を示す説明図であ

り、図において、３０は管理装置６でユーザ登録を行った際に登録されたユーザのユーザＩＤ、３１はユーザ認証のために用いる認証秘密情報、３２は管理装置６のＩＰアドレスを示す、管理手段情報としての管理装置ＩＰアドレスである。

【００１９】図４は管理装置６の有する機能を示す説明図である。図において、４０はユーザに発行するＩＣカード５に必要な情報の書き込みを行う、ＩＣカード書き込み処理機能である。４１は閉域通信に参加を希望するユーザの新規登録を行ない、各ユーザの閉域通信グループの登録を行うとともに、閉域通信グループ構成情報の表示、および変更を行う構成情報保存編集機能である。４２は端末暗号装置４に対して、閉域通信グループのグループＩＤ、および閉域通信用の暗号鍵を配送する暗号鍵配送機能である。

【００２０】次に動作について説明する。管理装置６は、あらかじめ次の処理を行っておくものとする。すなわち、まず最初に、その構成情報保存編集機能４１によって、当該閉域通信システムを利用することを希望する新規ユーザの登録を行う。登録が終わったユーザに対しては、そのＩＣカード書き込み処理機能４０を用いて、図３に示したユーザＩＤ３０、認証秘密情報３１、および管理装置ＩＰアドレス３２を、管理装置６において管理者によって決められたパスワード（初期パスワード）を用いて暗号化してＩＣカード５に書き込み、そのＩＣカード５を該当するユーザに発行する。ＩＣカード５を発行した後、各ユーザごとにそれが所属するグループのグループＩＤを定義しておく。

【００２１】この実施の形態１では、第１のユーザにはＩＣカード５ａを、第２のユーザにＩＣカード５ｂをそれぞれ発行し、これら第１のユーザと第２のユーザを同一の閉域通信グループに登録するものとする。

【００２２】次に、端末暗号装置４に対して閉域通信用のグループＩＤおよび暗号鍵を配送する動作について説明する。ここで、図５は端末暗号装置４へのグループＩＤおよび暗号鍵の配送動作を示すシーケンス図であり、この場合、ＩＣカード５ａの持ち主である第１のユーザ側の動作について示している。

【００２３】第１のユーザが管理装置６より発行してもらった、当該第１のユーザ用のＩＣカード５ａを端末暗号装置４ａのＩＣカードリーダ１９に差し込むと、当該端末暗号装置４ａのＩＣカード処理部２０は、その差し込まれたＩＣカード５ａの情報をＩＣカードリーダ１９を介して読み込み、ユーザ認証のためのパスワードの入力を促すパスワード要求１００を、ＰＣＩ／Ｆ２１を介して第１のユーザに送る。第１のユーザはこのパスワード要求１００に従って自身のパスワード１０１を入力する。入力されたパスワード１０１はＰＣＩ／Ｆ２１を介してＩＣカード処理部２０に送られ、ＩＣカード処理部２０は第１のユーザよりパスワード１０１が返送されてくると、それを用いてＩＣカードリーダ１９で読み出したＩＣカード５ａの内容の解読を行う。

【００２４】端末暗号装置４ａのＩＣカード処理部２０は、このＩＣカード５ａから読み込んだ第１のユーザのユーザＩＤ３０をパラメータ配送要求１０２とし、それを管理装置ＩＰアドレス３２に基づいて管理装置６のＩＰアドレス宛てに配送する。管理装置６は構成情報保存編集機能４１を用いて、この端末暗号装置４ａから受け取ったユーザＩＤ３０による検索を行って、第１のユーザが所属しているグループのグループＩＤとそれに対応する暗号鍵を決定する。管理装置６はさらに、それらグループＩＤと暗号鍵の情報を、そのユーザＩＤ３０に対応する認証秘密情報３１を用いて暗号化し、それをパラメータ配送暗号化１０３として端末暗号装置４ａに送る。

【００２５】このパラメータ配送暗号化１０３を受けた端末暗号装置４ａは、ＩＣカード５ａが保持している認証秘密情報３１を用いて受信したデータを復号し、グループＩＤおよび暗号鍵を得る。そして、管理装置６に対して確認応答１０４を返送するとともに、取得したグループＩＤおよび暗号鍵を用いて、自動学習処理部１４による動作テーブル１３の自動学習を行い、生成された動作テーブル１３による閉域通信を開始する。

【００２６】次に、上記動作テーブル１３による閉域通信の動作について説明する。ここで、図６は第１のユーザと第２のユーザとの間における閉域通信の動作を示すシーケンス図である。まず、この図６に示すように、第１のユーザより端末暗号装置４ａに対して、第２のユーザ宛ての通信データ１１０が入力される。なお、この通信データ１１０は、図２では図示を省略した通信データバッファ内に一旦保持される。通信データ１１０を受信した端末暗号装置４ａは内部の動作テーブル１３の検索を行う。初期の時点ではこの動作テーブル１３には、端末暗号装置４ａと端末暗号装置４ｂの間の通信処理方法は登録されていないので、端末暗号装置４ａは、図７に示す鍵探索バケット１１１を作成して端末暗号装置４ｂに送信する。

【００２７】図７は上記鍵探索バケット１１１のフォーマットを示すデータ構成図であり、鍵探索バケット１１１は、図示のように、種別２０１、宛先２０２、送信元２０３より成るヘッダ２００と、送信元アドレス２１１、宛先アドレス２１２、送信元端末暗号装置暗号鍵情報２１３、宛先端末暗号装置暗号鍵情報２１４より成るデータ部２１０によって形成されている。なお、この図７に示す例では、ヘッダ２００の種別２０１には探索バケットが、宛先２０２には端末暗号装置４ｂが、送信元２０３には端末暗号装置４ａが設定され、データ部２１０の送信元アドレス２１１には端末暗号装置４ａのアドレスが、宛先アドレス２１２には端末暗号装置４ｂのアドレスが、送信元端末暗号装置暗号鍵情報２１３には端

末暗号装置４ａの持つ暗号鍵のＩＤである１が設定されている。また、この端末暗号装置４ｂに送信される鍵探索パケット１１１では、端末暗号装置４ａと端末暗号装置４ｂの間の通信処理方法が登録されていないので、宛先端末暗号装置暗号鍵情報２１４には何も設定されていない。

【００２８】端末暗号装置４ｂではこの鍵探索パケット１１１を受信すると、図８に示すように、そのデータ部２１０の宛先端末暗号装置暗号鍵情報２１４に自身の暗号鍵のＩＤである１と２を設定する。端末暗号装置４ｂはこの宛先端末暗号装置暗号鍵情報２１４の設定が行われると、当該鍵探索パケット１１１のデータ部２１０をコピーして鍵探索応答パケット１１２を作成する。

【００２９】図９はこの鍵探索応答パケット１１２のフォーマットを示すデータ構成図であり、図７、図８に示した鍵探索パケット１１１と同様のヘッダ２００とデータ部２１０によって形成されている。ただし、ヘッダ２００の種別２０１には探索応答パケットが、宛先２０２には端末暗号装置４ａが、送信元２０３には端末暗号装置４ｂが設定され、データ部２１０では端末暗号装置４ｂのアドレスが送信元アドレス２１１となり、端末暗号装置４ａのアドレスが宛先アドレス２１２となっている。

【００３０】端末暗号装置４ｂは、生成した鍵探索応答パケット１１２の送信元端末暗号装置暗号鍵情報２１３に、自身の暗号鍵のＩＤである１または２と同じ暗号鍵のＩＤが設定されていないかどうか検索する。この場合、端末暗号装置４ａが鍵探索パケット１１１に設定した、当該端末暗号装置４ａの暗号鍵のＩＤである１がコピーされて、鍵探索応答パケット１１２の送信元端末暗号装置暗号鍵情報２１３に設定されている。このように、端末暗号装置４ｂの暗号鍵のＩＤである１が、鍵探索応答パケット１１２の送信元端末暗号装置暗号鍵情報２１３に設定されているので、端末暗号装置４ｂは自身の動作テーブル１３に、端末暗号装置４ａと端末暗号装置４ｂの間の通信データをＩＤが１の暗号鍵で暗号／復号することを登録するとともに、その鍵探索応答パケット１１２をヘッダ２００の宛先２０２に従って、端末暗号装置４ａに送信する。

【００３１】端末暗号装置４ａは、この鍵探索応答パケット１１２を受信すると、その宛先端末暗号装置暗号鍵情報２１４に自身の暗号鍵のＩＤである１と同じ暗号鍵のＩＤが設定されているかどうかを検索する。この場合、当該宛先端末暗号装置暗号鍵情報２１４には端末暗号装置４ｂが設定した暗号鍵のＩＤである１と２の２つが設定されている。従って、端末暗号装置４ａは自身の動作テーブル１３に、端末暗号装置４ａと端末暗号装置４ｂの間の通信データをＩＤが１の暗号鍵で暗号／復号することを登録する。

【００３２】端末暗号装置４ａは通信データバッファ内に保持しておいた第１のユーザからの通信データ１１０を、暗号／復号処理部１０において、動作テーブル１３の内容に従って、ＩＤが１の暗号鍵を用いて暗号化して暗号通信データ１１３を生成し、それを端末暗号装置４ｂ宛てに送信する。また、受信した鍵探索応答パケット１１２のヘッダ２００では、その宛先２０２が当該端末暗号装置４ａになっているので、端末暗号装置４ａはこの鍵探索応答パケット１１２をその廃棄処理部１２において廃棄する。

【００３３】一方、端末暗号装置４ａで暗号化された暗号通信データ１１３を受け取った端末暗号装置４ｂは、自身の動作テーブル１３の内容に従って暗号／復号処理部１０において、ＩＤが１の暗号鍵を用いてその暗号通信データ１１３を通信データ１１０に復号し、ＰＣＩ／Ｆ２１より第２のユーザに提示する。

【００３４】同様に、第２のユーザから第１のユーザへの通信データ１１４は、端末暗号装置４ｂでその動作テーブル１３の内容に従って、ＩＤが１の暗号鍵によって暗号化され、暗号通信データ１１５として端末暗号装置４ａに送られる。端末暗号装置４ａではその暗号通信データ１１５を、自身の動作テーブル１３の内容に従ってＩＤが１の暗号鍵により復号し、復号した通信データ１１４を第１のユーザに提示する。

【００３５】次に、このようにして第２のユーザと閉域通信を行っている第１のユーザが、その作業場所を変えた場合の動作について説明する。第１のユーザは作業場所を変える場合、元の作業場所に備えられた端末暗号装置４ａのＩＣカードリーダ１９から、自身に発行されたＩＣカード５ａを抜き取り、それを移動先の作業場所に備えられた端末暗号装置４ｃのＩＣカードリーダ１９に挿入する。端末暗号装置４ｃはＩＣカード５ａが挿入されると、そのユーザＩＤ３０より当該第１のユーザが所属しているグループＩＤを管理装置６より送ってもらう。これによって閉域通信の対象となるユーザ認証を行い、第１のユーザが同一の閉域通信グループのユーザであると認識されると、端末暗号装置４ｂのＩＣカードリーダ１９にＩＣカード５ｂを挿入した第２のユーザとの閉域通信が可能になる。

【００３６】以上のように、この実施の形態１によれば、ユーザにユーザＩＤ３０、認証秘密情報３１、管理装置ＩＰアドレス３２を保持したＩＣカード５を発行して、ＩＣカード５ａの持ち主である第１のユーザと、ＩＣカード５ｂの持ち主である第２のユーザを同一の閉域通信グループに登録し、第１のユーザがＩＣカード５ａを端末暗号装置４ａに挿入すると、管理装置６から第１のユーザが所属しているグループＩＤを配送しているので、同一の閉域通信グループに属する第２のユーザとの閉域通信が可能になり、また、第１のユーザがその作業場所を変えた場合でも、移動先の作業場所に設置された端末暗号装置４ｃにＩＣカード５ａを挿入すると、管理

装置６からその端末暗号装置４ｃに対して第１のユーザが所属しているグループＩＤが配送されるため、ユーザの使用する端末（端末暗号装置）が固定されることがなくなり、端末に依存することなく第２のユーザとの間で同一の閉域通信が可能になるなどの効果が得られる。

【００３７】実施の形態２．次に、この発明の実施の形態２による閉域通信システムについて説明する。この実施の形態２は、閉域通信終了時の処理に関するものであり、図１０はそのようなこの実施の形態２における、端末暗号装置４のＩＣカードリーダ１９からＩＣカード５を抜き取った場合の動作を示すシーケンス図である。

【００３８】まず、この図１０に示すように、当該閉域通信を終了したい第１のユーザが端末暗号装置４ａのＩＣカードリーダ１９よりＩＣカード５ａを抜き取る。端末暗号装置４ａではこのＩＣカード５ａの抜き取りを、そのＩＣカード処理部２０で検出すると、管理装置６に対してＥＮＤＴＲＡＰ１２０を送信する。このＥＮＤＴＲＡＰ１２０を受信した管理装置６はＥＮＤＴＲＡＰ応答１２１を生成し、それを端末暗号装置４ａに返送する。管理装置６からこのＥＮＤＴＲＡＰ応答１２１を受け取った端末暗号装置４ａは、内蔵する動作テーブル１３を消去するとともに、当該閉域通信を終了する。このようにして閉域通信を終了した端末暗号装置４ａは、その透過中継処理部１１を用いて、閉域通信グループに属さない一般の端末と同様の動作を行う。

【００３９】このように、この実施の形態２によれば、端末暗号装置４はそのＩＣカードリーダ１９よりＩＣカード５ａを抜き取るだけで動作テーブル１３が消去されるため、簡単に閉域通信を終了して、一般の端末と同様の動作を行うことが可能となる効果が得られる。

【００４０】実施の形態３．次に、この発明の実施の形態３について説明する。この実施の形態３はユーザ側からの、管理装置６で決定したパスワードの変更処理に関するものである。このパスワードの変更はユーザによって、ＰＣＩ／Ｆ２１を介して会話形式で行われ、その制御はパスワード変更手段として機能するＩＣカード処理部２０によって処理される。すなわち、端末暗号装置４のＩＣカードリーダ１９にＩＣカード５が挿入されると、ＩＣカード処理部２０よりＰＣＩ／Ｆ２１を介して、パスワードの入力がユーザに対して要求される。ユーザによってパスワードが入力されると、ＩＣカード処理部２０はＰＣＩ／Ｆ２１を介して、パスワードの変更に関するメニューを表示する。このメニューを参照したユーザが変更ありを選択すると、ＩＣカード処理部２０はＰＣＩ／Ｆ２１を介して、新たなパスワードの入力を要求する。ユーザによって新たなパスワードが入力されると、ＩＣカード処理部２０はそれに基づくパスワードの変更処理を行う。

【００４１】以上のように、この実施の形態３によれば、管理装置６で決定したパスワードを、ユーザ側で必要に応じて、会話形式による簡単な操作で変更することが可能になり、セキュリティの向上が図れるという効果が得られる。

【００４２】実施の形態４．なお、上記各実施の形態では、端末暗号装置４は管理装置６からグループＩＤおよび暗号鍵の配送を受け、配送された情報をもとに動作テーブル１３を自動学習する場合について説明したが、管理装置６が各端末暗号装置４の動作テーブル１３を何らかの手段であらかじめ保持していれば、パラメータ配送で上記動作テーブル１３を直接各端末暗号装置４に配送するようにしてもよく、上記各実施の形態と同様の結果を得ることができる。

【００４３】また、上記各実施の形態では、端末の機能と暗号装置の機能を併せ持った端末暗号装置４を用いて閉域通信システムを構成したものについて説明したが、従来の場合と同様に、端末暗号装置４に代えて端末と暗号装置を個別に設けるようにしてもよく、上記各実施の形態と同様の結果を奏する。

【００４４】さらに、上記各実施の形態では、管理装置６から端末暗号装置４に配送したユーザのグループＩＤおよびそれに対応する暗号鍵の情報を、通信相手の端末暗号装置４との間で直接交換して、動作テーブル１３の自動生成するものについて説明したが、中継装置を介して交換するようにしてもよく、上記各実施の形態と同様の結果を奏する。

【００４５】

【発明の効果】以上のように、この発明によれば、ユーザ認証のための情報を保持する外部記憶媒体をユーザに持たせ、当該情報をもとに生成した動作テーブルの内容に従って、通信データの暗号および復号の処理を行うように構成したので、ユーザは使用する端末（処理手段）が固定されることがなくなり、任意の端末を用いて閉域通信を行うことが可能な閉域通信システムが得られる効果がある。

【００４６】この発明によれば、外部記憶媒体にユーザＩＤ、認証秘密情報、管理手段情報を保持させ、当該外部記憶媒体を挿入した時、それが保持する情報をもとに、管理手段より処理手段に動作テーブルを配送させるように構成したので、外部記憶媒体が保持する情報をもとに配送された動作テーブルに従って閉域通信を行うことが可能となり、作業場所が変わっても異なる端末（処理手段）によって同一の閉域通信を行うことができるという効果がある。

【００４７】この発明によれば、ユーザのグループＩＤとそれに対応する暗号鍵を管理手段から処理手段に配送して、それらの情報を通信相手の処理手段または中継装置との間で交換することで、動作テーブルの自動生成を行うように構成したので、上記グループＩＤを用いた自動学習により生成された動作テーブルに従って閉域通信を行うことが可能となり、作業場所が変わっても異なる

11

端末（処理手段）によって同一の閉域通信を行うことができるという効果がある。

【００４８】この発明によれば、外部記憶媒体が抜き取られると、保持している動作テーブルの消去を行うように構成したので、外部記憶媒体を挿入した時には閉域通信を行い、外部記憶媒体を抜き取った時には一般の通信を行うことが可能になるという効果がある。

【００４９】この発明によれば、管理手段において決定した、外部記憶媒体の内容を暗号化するためのパスワードを、処理手段にて変更可能に構成したので、ユーザ側でこのパスワードを必要に応じて変更することにより、セキュリティを向上させることができるという効果がある。

【００５０】この発明によれば、外部記憶媒体としてＩＣカードを用いるように構成したので、外部記憶媒体の取り扱いが容易となり、その管理もしやすいものになるなどの効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１による閉域通信システムの構成を示すシステム構成図である。

【図２】　実施の形態１における端末暗号装置の内部構成を示すブロック図である。

【図３】　実施の形態１における管理装置よりユーザに発行されるＩＣカードに書き込まれる情報を示す説明図である。

【図４】　実施の形態１における管理装置の有する機能を示す説明図である。

12

＊【図５】　実施の形態１における端末暗号装置へのグループＩＤおよび暗号鍵の配送動作を示すシーケンス図である。

【図６】　実施の形態１におけるユーザ間の閉域通信の動作を示すシーケンス図である。

【図７】　実施の形態１における宛先端末暗号装置暗号鍵情報が未設定の鍵探索バケットのフォーマットを示すデータ構成図である。

【図８】　実施の形態１における宛先端末暗号装置暗号鍵情報が設定済みの鍵探索バケットのフォーマットを示すデータ構成図である。

【図９】　実施の形態１における鍵探索応答バケットのフォーマットを示すデータ構成図である。

【図１０】　この発明の実施の形態２におけるＩＣカードを抜き取った場合の動作を示すシーケンス図である。

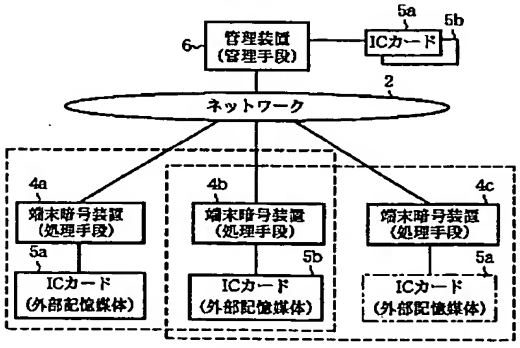
【図１１】　従来の閉域通信システムの構成を示すシステム構成図である。

【図１２】　従来の閉域通信システムにおける暗号装置の内部構成を示すブロック図である。

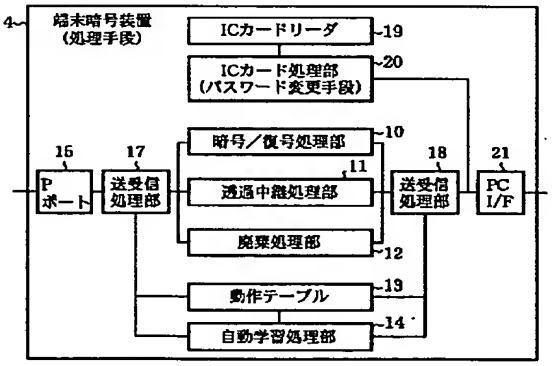
【符号の説明】

２　ネットワーク、４，４ａ，４ｂ，４ｃ　端末暗号装置（処理手段）、５，５ａ，５ｂ　ＩＣカード（外部記憶媒体）、６　管理装置（管理手段）、１３動作テーブル、２０　ＩＣカード処理部（パスワード変更手段）、３０　ユーザＩＤ、３１　認証秘密情報、３２　管理装置ＩＰアドレス（管理手段情報）、１１０，１１４　通信データ。

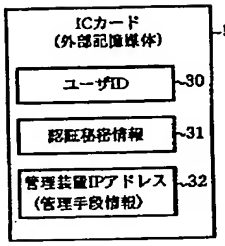
【図１】



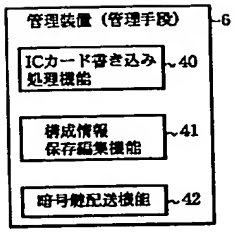
【図２】



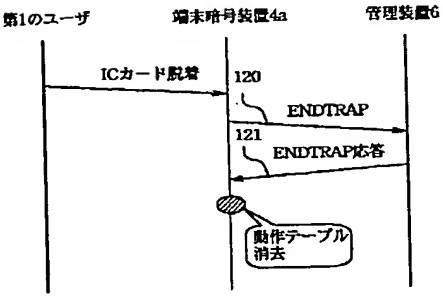
【図３】



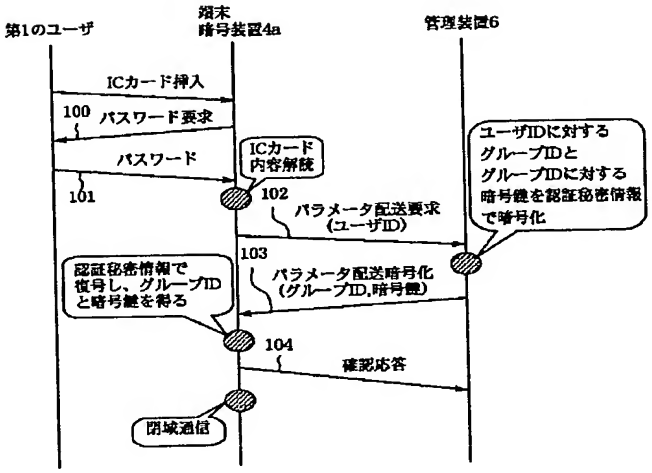
【図４】



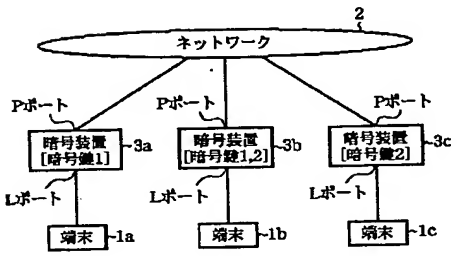
【図１０】



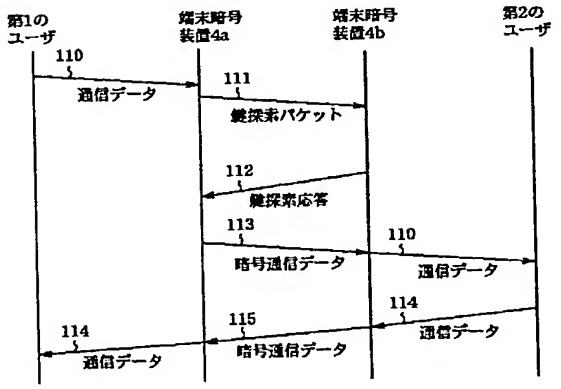
【図５】



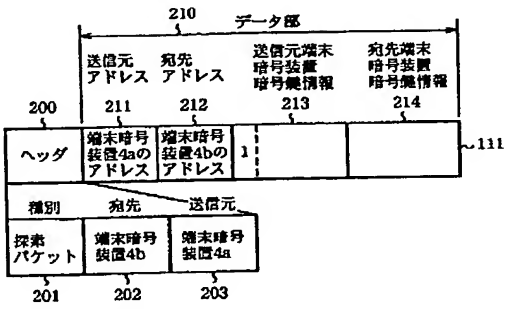
【図１１】



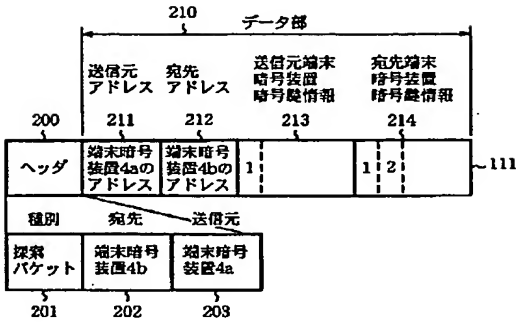
【図６】



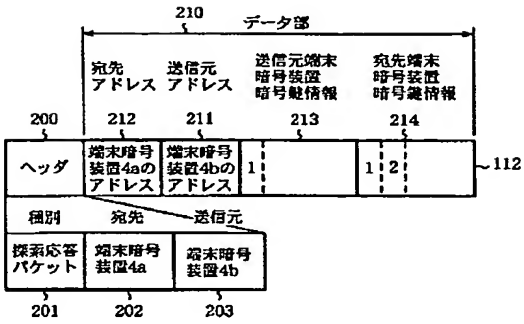
【図７】



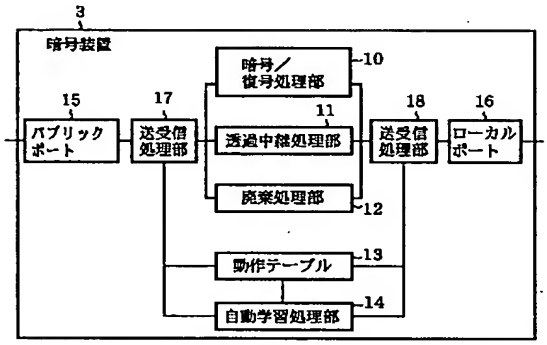
【図８】



【図９】



【図１２】



フロントページの続き

(72)発明者　渡邊　晃
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　宮川　明子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　後沢　忍
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　西條　智幸
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　岡　克也
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　瀬口　有美
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA07 AA16 EA01 EA06 EA17
EA22 KA01 MA02 MA06 NA03
NA05 NA20 NA35 PA00
5K030 GA15 GA16 HC01 HC13 KA01
5K033 AA08 DA01 DB10 DB20